CYBER SECURITY NEWS
Vol. 6 | Issue 8
August 2021

Page 2 | Page 3 | Page 4 | Challenge | Closing

Welcome to the TXDPS Cyber Security Newsletter!

Cyber criminals use every opportunity to try to scam people out of money. With the Advance Payments of the Child Tax Credit going out to eligible taxpayers, the IRS warns folks to be aware that thieves may use these payments as bait.

By now, most eligible parents will already have had a deposit hit their bank account without taking any action whatsoever. The IRS is using bank information already on file from 2019 and 2020 tax returns to make the automatic deposits. No additional action is necessary.

So, what should you watch out for?

1. Be wary of anyone asking for personal information

Be alert to criminals who ask you, by phone, email, text – or even on social media, to verify your information so you can get advance Child Tax Credit payments.

Remember…the IRS does not initiate contact with taxpayers by email, text messages or social media channels to request personal or financial information.

When it comes to phone calls, remember the IRS does not leave pre-recorded, urgent or threatening messages. For example, if you get a voice mail saying a warrant will be issued for your arrest… this is not the IRS.

2. Don't click on any suspicious links that claim to be from the IRS

The IRS says that another red flag is someone who is trying to shake you down: if they ask for payment via a gift card, wire transfer or cryptocurrency.

Clicking on links in unsolicited emails or websites posing as legitimate sites, and offering up any information could lead to theft, tax fraud, and identity theft.

3. Contact the FTC and IRS if you notice anything wrong

If you believe you've been targeted by a Child Tax Credit scam, follow the cardinal rule of personal safety by never sharing sensitive data with an unverified source. Triple-check the URL on any IRS webpage you visit, as these are easily spoofed. Note that all authentic government sites will end in .gov. Finally, report all suspicious activity to the IRS and the FTC immediately.

To learn more about the advance child tax credit—including who is eligible and how to provide your information to the IRS for this credit, and to learn more about protecting yourself against scams, go to IRS.gov/childtaxcredit2021 and IRS.gov/scams.

Cyber Risk Management

For this month's highlight of cyber risk controls, we are taking a look at how cybersecurity risk translates directly into business risk for your division and business operations. To do so, we will take a look at the tenets of keeping our data safe, by ensuring we are following the CIA. No...not that CIA!

Here, we will discuss the importance of the Confidentiality, the Integrity, and the Availability of data. Together, these three will ensure that the data you use to conduct your daily business is kept secure, correct, and available for you to use whenever you need.

In fact, when Cyber Risk conducts a risk assessment, part of what we look at is the potential impact to DPS operations if the risk were to be realized, and we look at this in terms of confidentiality, integrity, and availability of the system and data. So let's dig a bit into each of these.

Confidentiality

Here at DPS, we work with a lot of sensitive information that Texans trust us with. That means it is our responsibility to ensure the data is kept secure and not given out to unauthorized parties. In order to help us keep all the data secure, make sure to use technical protections like encryption, and use passwords and permissions to ensure only employees who need to know information will have access to it.

Integrity

Beyond just keeping the information secure, there is also the responsibility to ensure the data we have is accurate and has not been tampered with. In order for you to conduct your business, you need to know that all the information you are working with is reliable and can be trusted to be correct. Otherwise, you cannot perform your business functions. To keep the data accurate and reliable, be careful about the changes you make to any system.

Availability

Considering the two elements above, even if all the data is kept confidential and has integrity, that doesn't mean anything unless you are able to access it for your essential business functions. Availability is important in ensuring that the people who need access to the data can always have access, necessitating disaster recovery systems and plans.

Social Media Safety

I'm sure you have heard about the importance of considering what you share on social media, but this topic is so important, it is worth a refresher.

US-CERT's Summertime Tips for Online Safety and Security

The United States Computer Emergency Readiness Team, or US CERT, has developed some guidelines for Americans as you use social media and other online applications. Read on to learn how to protect yourself, friends, and family from being taken advantage of online.

How can you protect yourself?

- **Limit the amount of personal information you post** - Do not post information that would make you vulnerable, such as your address or information about your schedule or routine. If your connections post information about you, make sure the combined information is not more than you would be comfortable with strangers knowing. Also be considerate when posting information, including photos, about your connections.
- **Remember that the internet is a public resource** - Only post information you are comfortable with anyone seeing. This includes information and photos in your profile and in blogs and other forums. Also, once you post information online, you can't retract it. Even if you remove the information from a site, saved or cached versions may still exist on other people's machines.
- **Be wary of strangers** - The internet makes it easy for people to misrepresent their identities and motives. Consider limiting the people who are allowed to contact you on these sites. If you interact with people you do not know, be cautious about the amount of information you reveal or agreeing to meet them in person.
- **Be skeptical** - Don't believe everything you read online. People may post false or misleading information about various topics, including their own identities. This is not necessarily done with malicious intent; it could be unintentional, an exaggeration, or a joke. Take appropriate precautions, though, and try to verify the authenticity of any information before taking any action.
- **Evaluate your settings** - Take advantage of a site's privacy settings. The default settings for some sites may allow anyone to see your profile, but you can customize your settings to restrict access to only certain people. There is still a risk that private information could be exposed despite these restrictions so don't post anything that you wouldn't want the public to see. Sites may change their options periodically so review your security and privacy settings regularly to make sure that your choices are still appropriate.
- **Be wary of third-party applications** - Third-party applications may provide entertainment or functionality, but use caution when deciding which applications to enable. Avoid applications that seem suspicious, and modify your settings to limit the amount of information the applications can access.
- **Use strong passwords** - Protect your account with passwords that cannot easily be guessed. If your password is compromised, someone else may be able to access your account and pretend to be you.
- **Check privacy policies** - Some sites may share information such as email addresses or user preferences with other companies. This may lead to an increase in spam. Also, try to locate the policy for handling referrals to make sure that you do not unintentionally sign your friends up for spam. Some sites will continue to send email messages to anyone you refer until they join.
- **Keep software, particularly your web browser, up to date** - Install software updates so that attackers cannot take advantage of known problems or vulnerabilities. Many operating systems offer automatic updates. If this option is available, you should enable it.
- **Use and maintain anti-virus software** - Anti-virus software helps protect your computer against known viruses, so you may be able to detect and remove the virus before it can do any damage. Because attackers are continually writing new viruses, it is important to keep your anti-virus software up to date.

Want to learn more? Visit US-CERT for tips on protecting yourself on social media here: [Staying Safe on Social Networking Sites | CISA]

In the News

Kaseya ransomware attack: 1,500 companies affected, company confirms

(Liam Tung | July 6th, 2021)

Enterprise tech firm Kaseya has confirmed that around than 1,500 businesses were impacted as a result of an attack on its remote device management software, which was used to spread ransomware.

It appears that the attackers carried out a supply chain ransomware attack by leveraging a vulnerability in Kaseya's VSA software against multiple managed service providers (MSP) – and their customers.

"To date, we are aware of fewer than 60 Kaseya customers, all of whom were using the VSA on-premises product, who were directly compromised by this attack. While many of these customers provide IT services to multiple other companies, we understand the total impact thus far has been to fewer than 1,500 downstream businesses. We have not found evidence that any of our SaaS customers were compromised," Kaseya said in an update on the attack.

The attackers exploited a previously unknown flaw in Kaseya's VSA software, which is used by MSPs and their customers. VSA is remote monitoring and management software, which is used to manage endpoints, such as PCs, servers and cash registers, as well as manage patching and security vulnerabilities.

On Sunday, the actors asked for $70 million in exchange for a universal decryption tool that would supposedly resolve the REvil issue for Kaseya and its customers.

Some victims, such as Swedish supermarket Coop remained closed for business on Monday due to the attack. The company is currently working to replace its affected checkout systems at multiple stores, it said in a statement on Monday.

Kaseya noted that it had not received reports of VSA customers that had been compromised since Saturday. It says that no other Kaseya products were compromised.

While Kaseya's software-as-a-service (SaaS) line of VSA was not affected, its servers were taken down during the incident response and remain offline today.

Kaseya has developed a patch for customers running VSA on their own servers. A patch should be available with 24 hours after its SaaS servers are brought back online, which it estimates will happen July 6, between 2 PM and 5 PM EDT, Kaseya said in an update.

Full Story: https://www.zdnet.com/article/kaseya-ransomware-attack-1500-companies-affected-company-confirms

A Few More Cyber News Stories:

Windows Hello Bypass Fools Biometrics Safeguards in PCs
https://threatpost.com/windows-hello-bypass-biometrics-pcs/167771/

Nearly Every Organization Has Had an Insider-Caused Data Breach in the Last Year
https://blog.knowbe4.com/nearly-every-organization-has-had-an-insider-caused-data-breach-in-the-last-year

Cryptographers unearth vulnerabilities in Telegram's encryption protocol
https://www.cyberscoop.com/telegram-app-security-encryption/

CYBER CHALLENGE

The Weakest Link

This Month's Challenge

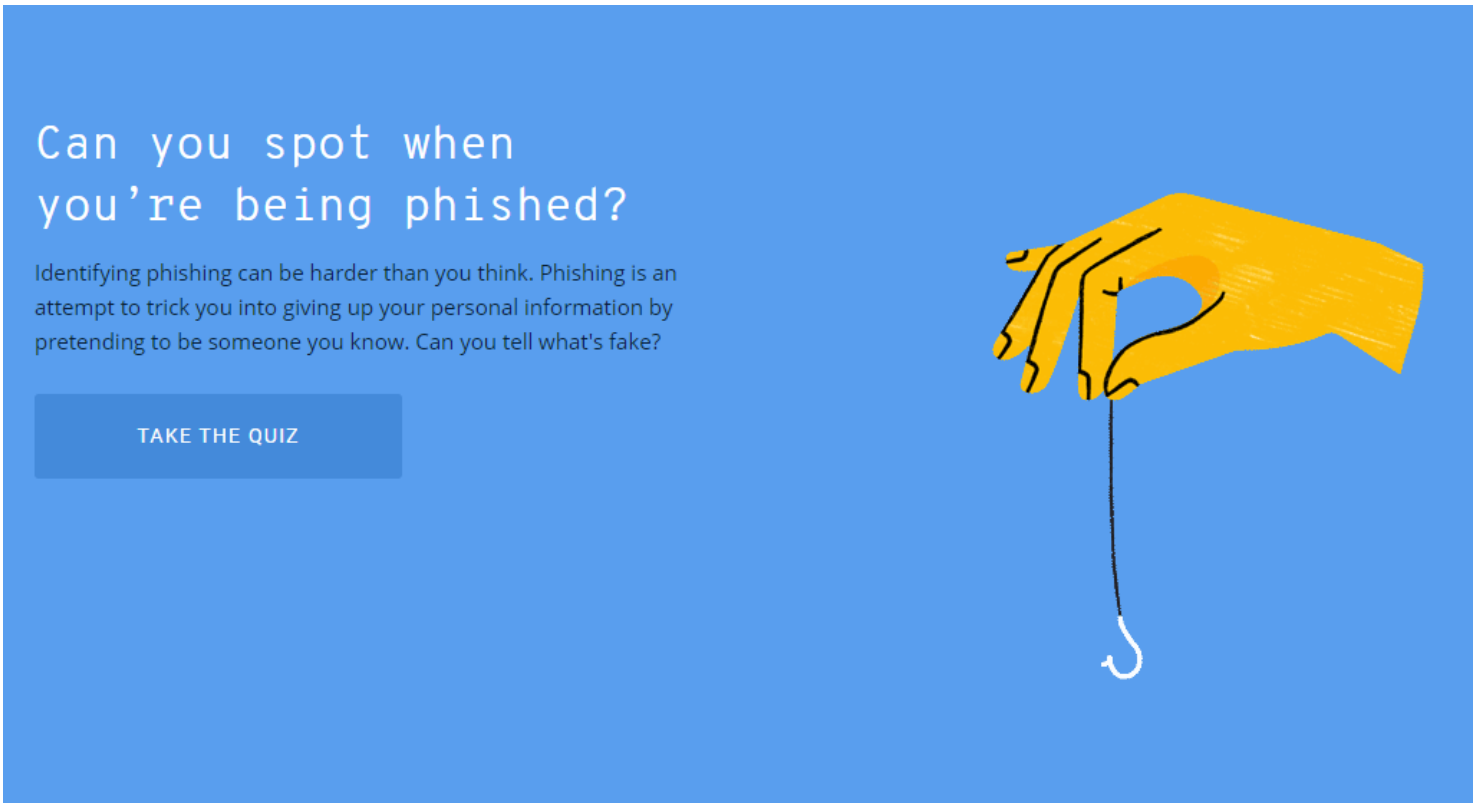
Phishing is one of the most commonly encountered cybersecurity risks that you will face. So let's see how well you do at spotting them!

For this month's challenge, let's play a game developed by Google in partnership with Jigsaw.

Are you able to tell the difference between phishing and legitimate emails? Look closely, they may be very convincing!

Let me know your score at the end. And please feel free to share anything you struggled with; it'll only help me to know where we can bolster our cyber security awareness and help you better spot phishing.

You got this! (~15 min. to complete)



</Closing Comments>

As we close this month's newsletter, we'd like to give a quick shout out to those of you who took the time to engage with our cyber challenge. We fully appreciate you taking a few minutes out of your day to engage with us. Please keep doing so; and get others to join you.

A big THANK YOU to:

Regina S.
Debra L.
Kari R.
Dax R.
Chris B.
Lane T.
Barbara R.
Eddy H.
Slobodanka D.
Brenda D.
Keith G.
Denise L.
Jessica B.

If we missed you, let us know!

Hey everyone! I am Cory Chang, and I am one of the interns here at DPS Cyber Security. I spent a bit of time this past week to write this newsletter, and I hope you enjoyed the selection of tips and news articles I chose for this month. I really appreciate you spending the time to read through the newsletter, and continuing to be cyber aware to protect all of us here at DPS.

As always, if you have any feedback, we would be happy to hear from you! You can email any thoughts, questions, or comments you have about cyber security and/or the newsletter to Eric Posadas at eric.posadas@dps.texas.gov.

Thank you again for what you do at DPS, and remember to stay vigilant about any potential cyber threats!

- Cory Chang

Share and Connect

Newsletter Archive Cyber SharePoint